Under Cover of Darkness

Practical considerations for (legally) breaking and entering.

Tom Follow
Feb 12, 2019 · 9 min read

I work in a Red Team. My job, broadly, is to replicate the actions of a "bad guy" and attack my clients' organisations. My clients want to know how bad guys might break in, but they don't want to end up on the front of the Wall Street Journal in the process.

Introducing the post with a serious hacking photo — Photo by Nahel Abdul Hadi on Unsplash

My background is in Computer Systems Engineering — there are certain elements of "breaking in" that I feel a natural affinity for. Exploiting poorly patched routers, abusing PHP web services and reverse engineering desktop software are all firmly within my remit — these things involve "computers" and "sitting in dark rooms" — I can relate to these things.

During my second Red Teaming engagement at TSS my manager called for volunteers to learn the ropes of physical access. That is, breaking and entering. Not truly understanding the implications of my decision, I put my hand up. Now "Computers" and "dark rooms" were to become "locked doors", "suspicious guards" and "places in which I could feasibly be arrested".

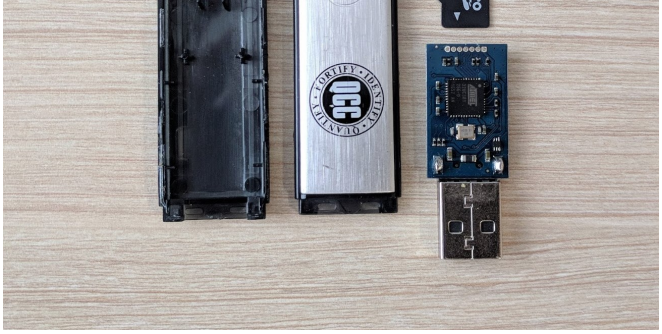
I've done this a number of times now but the ~~fear, nerves,~~ thrill of it never really goes away. There's a lot that I could say on the topic but in this post I want to discuss one of the fundamental considerations — "when".

. . .

Breaking In

Other questions like "how" and "why" you might break into a building are easy questions — they have relatively concrete answers. Anyone breaking into a building without a watertight "why" is probably not doing so legally, and "how" generally falls within the realm of definitive answers to technical problems.

"when" is not definitive, "when" doesn't always have a right answer, "when" is artistic, malleable, fragile, like a Frank Lloyd Wright ice-cream Jenga tower, and no less messy if you screw it up.



A USB Rubber Ducky from Hak5. It looks like a normal USB thumb drive (this one is disassembled) and it is, sort of. When plugged into a computer this nifty gadget will act as a keyboard, sending hundreds of keystrokes per second. The applications of this are only limited by the attacker's creativity. A common use case leverages the ultra-fast typing to quickly spawn a shell via cmd.exe (especially if spawning that shell requires typing out several lines of PowerShell — machines can typically do that faster than you can). A Ducky set up to perform such an attack could then be used to opportunistically compromise unlocked computers, or the device could be dropped near to your target — perhaps someone will plug it in for you.

Night Entry

Presumably, if I were to be discovered having broken into a building by your average office worker, chances are, they would call security. Were security not forthcoming (or existent) they might call their manager, colleague, maybe even the police. Most people don't enjoy being arrested [citation needed] — myself included (although I haven't technically tried it). I also don't want to waste the time and resources of law enforcement (we have strategies to avoid this at all costs) so when I began my ethical cat-burgling career, the concept of getting caught was about as appealing as gargling a pint of bees … or eating some coriander.

Solution — If we go in at night, we won't get caught? No-one can see us. Perfect.

> *"Easy."*
> *- Me, prior to giving this issue any thought at all.*

No.

Entering your target building at night time does have certain benefits. Namely:

- Once inside the building you're less likely to be disturbed, allowing you to sweep for valuable information, keys, computers, etc.
- If you aren't disturbed, you can probably spend a really long time (all night, for example) in the target building. Assuming that this yields some value to the operation.
- You feel like James Bond.

But there are also some pretty significant downsides:

- You're more likely to trigger an alarm. Motion sensors firing at night are usually a really bad sign. Security guards are likely to respond.
- If someone is watching CCTV around the building's exterior it's likely that you'll be noted on approach the building. This depends somewhat on the geometry of the approach but be prepared for someone to have clocked you going in.
- Night guards dedicated to a specific building are likely to conduct walk-arounds. If this is the case then you'll need to take extra care not to be detected.
- 24/7 security contractors are often tasked with patrolling multiple sites on any given night. This means that there will be periods of the night during which it's very risky for you to be turning on lights or moving near windows. It pays in this scenario to have someone on the outside, watching for movement.
- The coffee machine is more likely to be turned off at night.

USB Armoury — A system-on-chip computer. A staple of my physical red teaming toolkit. This one is configured to run a Debian operating system, a DHCP server and the open source "Responder" attack tool (https://github.com/lgandx/Responder). When plugged into a USB port, it emulates an ethernet device over USB, it then attempts to attack local name resolution protocols commonly used by Windows. A successful attack gives us a password hash and an account name. We can then attempt to crack these offline using a password recovery tool such as Hashcat. Read about this in detail here — https://room362.com/post/2016/snagging-creds-from-locked-machines/

Day Entry

Day entry, as the name suggests, involves entering a building during the day. On the surface, this seems like a poorly conceived idea; thieves and brigands tend not to commit robberies in broad daylight — the likelihood of being detected is generally too high — the risk to reward isn't worth it.

> *People expect bad guys to be dressed in black and wearing balaclavas, they don't expect bored looking office workers carrying sandwiches.*

But we're not thieves — well, not in the conventional sense. If we're trying to leverage physical access to further digital access, then typically we're trying to get things IN to a target, rather than out. And people tend to be marginally less suspicious of a bored looking individual wearing crumpled office clothes and carrying a sandwich than they do of people running around wearing balaclavas, holding black duffel bags and brandishing baseball bats [citation needed]. What I'm getting at here is that people *expect* bad guys to be dressed in black and wearing balaclavas, they don't *expect b*ored looking office workers carrying sandwiches.

A key component of Red Teaming, and more specifically social engineering, is our ability to exploit the trust boundaries and assumptions of others.

Consider this situation: you work in a large, open plan office. Your local workforce numbers around 100 people, with more working at smaller offices interstate. Your office has hot desks for travelling workers and consultants.

Now consider that you see an unfamiliar face in the office. Someone that you don't recognise is sitting at a laptop, they're wearing a pass of some kind (although you can't see the ID card), they're eating a banana and drinking a cup of tea.

Do you call the police?

I'm going to assume for the sake of brevity that you answered "no" to the previous question. You don't call the police because it would be patently absurd, and your sanity might be called into question by your peers.

Photo by Andrew Neel on Unsplash

You might ask the person who they are and why you haven't seen them before. But if the person answers that they're "Susan from marketing" and that they're from out of town, are you really going to push the issue to the point of involving management and law enforcement? Unlikely.

Is this person meant to be here? Are they about to steal a NetNTLMv2 hash for your domain administrator from account? Or are you just not familiar with Susan from Marketing?

Statistically, it's just far more likely that you haven't met Susan from marketing than it is for Susan to be working for a foreign government intelligence service or shady criminal organisation. But it isn't impossible.

This assumption that someone who "looks" like they're meant to be somewhere is actually meant to be there is key during day entry (although it's key during all physical red teaming). The crowd present during the day can provide the perfect cover for a Red Teamer to move around an office, pretending to have legitimate business. The danger comes if they linger too long in one place, attracting unwanted attention. But if all that's required is that they plug a malicious network connected implant into an ethernet port, then a few minutes might be all they need.

Another undeniable advantage of the day entry is the alarm. The alarm is likely to be off during the day (how many people keep their building alarms on during the day?) No alarm means no immediate police response — that's what we want. A lot of other people in the target building also means that a guard watching CCTV will be much less likely to pay close attention to any one individual, this also works in our favour. Those same guards are also likely to assume that anyone within a building's secure perimeter during the work day is probably meant to be there. During the day, the guard has their hands full checking identities at the door. If you get past the door, well, you're probably in.

But what if you slip up? Well, I can speak from experience that it's uncomfortable. If you *are* directly challenged, you're put in a position where you have approximately 30 seconds to convince someone that you're totally cool and good and not at all suspicious. The longer this takes, typically the harder it is. Understanding your own physical reaction to direct confrontation is important here. Draw on what you know. Use your pretext. Don't panic. Be polite. Be boring.

Don't freeze and blurt out "I'M HERE TO FIX THE AIR-CONDITIONER" if you're dressed in a suit and carrying a laptop … and don't know how to fix an air-conditioner.

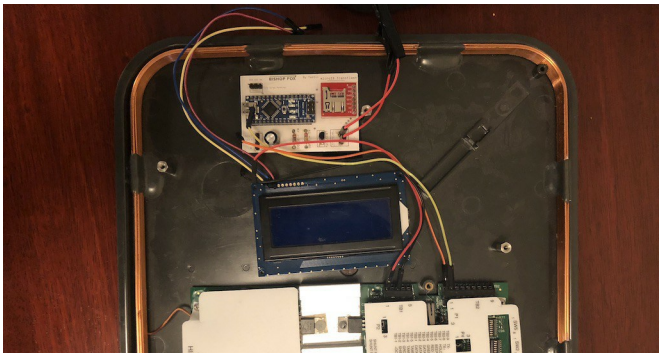
. . .

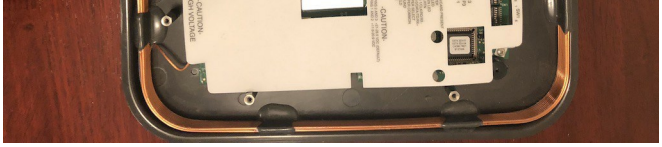
If pressed, I'd probably tell you that I'm a proponent of night entry, but honestly, I'm a proponent of controlled entry.

Night entry is great if you can leverage digital or RF attacks to disable alarms, cameras, access control systems and so on. That's the perfect scenario — but it requires higher intelligence and luck stats.

Day entry allows you to avoid the need for so much technical wizardry to bypass control systems, but it might require that you interact with people, so you're going to need to put a lot of points into luck and charisma.

So how do we get the best of both worlds?





A HID Global MaxiProx 125kHz card reader. You might typically see these devices in car parks — their intended use being to read cards from a distance. Combined with a Tastic RFID thief PCB (designed by Bishop Fox), an Arduino Nano and a micro SD card reader, we have a device that can steal card data from 1m away. Now we just need to loiter around some target employees and wait for the facility codes to roll in.

Cold Shoulder

The very end of the day represents a golden opportunity for physical access. The alarms are off, people are still at work (but not too many) and importantly, they're all thinking about going home, especially on Friday afternoon and *especially* on cold, rainy winter Friday afternoons. On these occasions, people mentally checked out hours ago so you're highly unlikely to be noticed (in general, don't quote me).

If you get into a target office after 5pm, you'll probably have at least an hour until the last person leaves. Hopefully they won't set the alarm without realising you're there. If they find you, tell them that you had a visitor escort but that you went to the kitchen/bathroom/printer and now you can't find them … just make sure you install your payload first.

Gut Feelings — Should I Stay Or Should I Go?

The advice given to me when starting down this path of clandestine role-play was "always trust your gut". It's good advice; if you see someone shoot a glance at you once, perhaps they're shy. If they do it twice and suddenly you don't feel comfortable — go. It's probably the right decision.

If you sit down at someone's desk and it feels natural to drink a cup of tea and read your phone, do that. If anything you're doing improves your ability to "act natural" you're helping yourself to blend in.

Just remember — only *you* know that you're not meant to be there. The guilty conscience weighs heavily when you break into a target, especially during the day. Consider your surroundings, try to get inside the heads of the unsuspecting office workers that you're trying desperately (calmly) to avoid eye contact with. Act on your gut, but always sanity check yourself: "Am I truly made? Or is this my guilty conscious". Quite often, you'll realise it's the latter.

Finally, be honest about when the job is done. It's fun to spend 12 hours in a target waiting for the *exact* right moment to plug in an evil network hop point. But if you can do it right away, do it right away.

You came here with a job to do.

So do it.

And try to look bored while you're doing it.

T.

> *All TSS red teaming is performed in a legal manner with full permission of the client.*
>
> *Tom is a principal penetration tester at TSS specialising in red teaming.*
>
> *TSS is a specialist cyber security company providing penetration testing, security assurance consulting and managed security services. More information is available at our website https://www.tsscyber.com.au.*

Security Infosec Hacking Red Team Penetration Testing

WRITTEN BY
Tom
Follow

@x86party | Red Teams | Coffee | Bouldering

TSS - Trusted Security Services

Follow

TSS is a leading cyber security company founded by former Australian Government security specialists. This blog is a way for TSS staff to contribute back to the security industry

Write the first response

More From Medium

Top on Medium

How I completely transformed my body in one year.

Matthew Boutte
Jan 14 · 11 min read ★

9K

Top on Medium

I Exercised 6 Times A Week For Two Months — Here's What I Learned

Refinery29 in Refinery29
Nov 1, 2019 · 8 min read ★

2.7K

Top on Medium

When a $100,000 Salary Isn't Enough

Adam Parsons in Making of a Millionaire
Dec 18, 2019 · 9 min read ★

2.3K

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade